采购编号： 常采公[2023]0192号

常州市12345平台升级改造项目信息安全风险评估服务项目合同书

甲　　方：常州市政务服务管理办公室

乙　　方：江苏瑞新信息技术股份有限公司

签订时间： 2023年09月

甲方：常州市政务服务管理办公室

乙方：江苏瑞新信息技术股份有限公司

地点：常州市政务服务中心 1-1 座 10 楼

签订时间：2023 年 09 月

甲、乙双方根据常采公[2023]0192 号的常州市 12345 平台升级改造项目信息安全风险评估服务项目采购结果及磋商文件的要求,经协商一致,达成如下采购合同:

一、总则

乙方按甲方要求，为甲方提供的 常州市 12345 平台升级改造项目信息安全风险评估服务项目 具体服务内容见下表（单位：万元）：

序	项目名称	内容说明	单价	数量	金额
1	常州市 12345 平台升级改造项目信息安全风险评估服务项目	信息安全风险评估服务[见附件一]	7.9 万元	1	7.9 万元
合计:79000 万元					

本合同金额为人民币大写： 柒万玖仟 元整，小写：¥ 79000 元 。

二、合同文件

下列文件是构成合同不可分割的部分，并与本合同具有同等法律效力，这些文件包括但不限于：

1、常采公[2023]0192 号招标文件。

2、乙方提交的投标文件。

3、乙方投标的其他资料及承诺。

三、质量保证和服务承诺

乙方所提供的服务必须符合国家有关标准和常采公[2023]0192 号采购文件（含技术说明）和投标文件的要求。

四、服务期限

服务期限：一年。

五、付款方式

本合同总金额为人民币大写：柒万玖仟元整，小写：¥ 79000 元 。

按照以下约定执行：合同签订后，甲方自收到乙方发票 15 日内支付合同总价的 50%作为预付款， 为人民币大写：叁万玖仟伍佰元整，小写：¥ 39500 元 。

项目通过大数据中心组织的验收后，甲方自收到乙方发票 15 日内一次性支付剩余 50%尾款，为人民币大写：叁万玖仟伍佰元整，小写：¥ 39500 元 。

六、保密条款

甲、乙双方另行签订保密协议作为本合同的附件，约定双方在保密方面的权益与义务及违约责任。服务期间甲方单位提供的资料，以及扫描分析结果，乙方用完即毁、不得留存。

七、违约责任

甲方无正当理由拒收该项目服务的，由甲方向乙方偿付合同总价款的 5%违约金，不可抗力除外；

甲方未按合同规定的期限向乙方支付款项的，每逾期 1 天甲方向乙方偿付欠款总额的 5%滞纳金，但累计滞纳金总额不超过欠款总额的 5%。

因财政拨付周期或支付进度等问题导致逾期付款，甲方不承担违约责任。

乙方未按合同的规定提供服务的，应按合同总价款的 5%向甲方承担违约责任。

八、不可抗力

甲、乙双方中任何一方，由于遭受战争、疫病、严重火灾、洪水、台风、地震或其它双方认为不可抗力事件致使无法履行合同时，或延长合同执行期，延长期应相当于不可抗力事件持续时间。

遭受不可抗力事件一方应尽快以传真方式通知另一方，并在不可抗力事件发生后 15 天内将有关当局出具的证明文件正本以快递方式寄出，供另一方审查确认。

一旦不可抗力事件终止或解除，由遭受不可抗力事件一方须以传真方式通知另一方，并寄出正本信件予以确认。

如不可抗力事件持续 2 个月以上，则双方尽力协商解决所引起的问题；如持续 3 个月以上，则任何一方有权终止部分或全部合同。

九、合同纠纷处理

本合同执行过程中发生纠纷，由甲乙双方协商解决，若协商不成，作如下 2 处理：

1、申请仲裁。选定仲裁机构为常州仲裁委员会。

2、提起诉讼。约定由采购人所在地法院管辖。

十、合同生效及其它

本合同经甲方、见证方和乙方三方签字盖章后生效。如有变动，必须经甲方、乙方协商一致，方可更改。本合同一式肆份，以中文书就，甲方、乙方各执二份。

十一、组成本合同的文件包括

1、合同主要条款和通用条款；

2、磋商文件和乙方的磋商响应文件；

3、成交通知书；

4、甲乙双方商定的其他必要文件。上述合同文件内容互为补充，如有不明确，由甲方负责解释。

附件一：服务内容

附件二：信息安全风险评估服务项目保密协议

附件三：外包单位网络安全承诺书

（此页无正文）

甲方：单位名称（章）：常州市政务服务管理办公室

单位地址：常州市政务服务中心 1-1 座 10 楼

法定代表人：

委托代理人：

电　话：

日　期：

乙方：单位名称（章）：江苏瑞新信息技术股份有限公司

单位地址：常州市新北区太湖东路 9-2 号三楼

法定代表人：

委托代理人：

电　话：

日　期：

附件一：服务内容

一、项目目标

为准确识别信息安全各种风险和威胁，规避或减少信息安全事件造成的不良影响和损失，常州市政务服务管理办公室拟采购信息安全风险评估项目，其中安全评估涉及常州市12345平台升级改造项目。

1.根据信息安全风险级别，运用科学方法和手段，系统地分析网络和信息系统所面临的威胁及其脆弱性，评估安全事件一旦发生可能造成的危害程度，提出针对性的信息安全解决方案和加固建议，为网络、软硬件系统的安全与稳定运行提供有力的保障。

2.通过专业的安全服务和管理，及时协助信息安全管理人员发现和处理服务范围内的设备及系统安全事故，提供有针对性的安全咨询及安全规划方案，最大限度保障网络和信息安全。

二、项目实施原则

1.保密原则

在运维过程中，需严格遵循保密原则，招标方与投标方签订保密协议，对服务过程中涉及到的任何用户信息未经允许不向其他任何第三方泄漏，以及不得利用这些信息损害用户利益。

2.互动原则

在整个运维过程中，强调用户的互动参与，每个阶段都能够及时根据用户的要求和实际情况对评估的内容、方式做出相关调整，进而更好的进行项目服务工作。

3.最小影响原则

工作应该尽可能小地影响系统和网络的正常运行，不能对业务的正常运行产生明显的影响（包括系统性能明显下降、网络阻塞、服务中断等），如无法避免，则应做出说明。

4.规范性原则

常州市大数据管理中心安全评估服务的实施必须由专业人员依照规范的操作流程进行，对操作过程和结果要有相应的记录，并提供完整的运维报告。

5.质量保障原则

在整个项目服务过程中，将特别重视项目质量管理。项目的实施将严格按照项目实施方案和流程进行，并由项目协调小组从中监督，控制项目的进度和质量。

三、测评技术要求

按照《GB/T 20984-2007》风险评估要求,对常州市 12345 平台升级改造项目上承载的数据、业务和应用等进行安全评估，明确信息系统存在的问题和不足，主要包括:

1.差距分析

通过、调查问卷、人员访谈、文档查看、现场勘查、人工检查、记录分析、技术测试、渗透测试等方式进行安全技术和安全管理方面的评估，判断安全技术和安全管理的各个方面，给出差距分析结果，提出信息系统的安全保护需求。

2.风险评估

对常州市 12345 平台升级改造项目的重要资产进行风险评估，分析并确定不能接受的安全风险，然后确定额外安全措施并判断对超出等级保护基本要求部分实施额外安全措施的必要性，提出信息系统的额外安全保护需求。

四、技术标准

1.《信息安全风险评估规范》（GB/T 20984-2007）

2.《信息安全风险管理指南》（GB/Z 24364-2009）

3.《信息系统安全等级保护基本要求》（GB/T 22239-2008）

4.《信息安全管理实用规则》（GB/T 22081-2008）

5.《信息系统安全管理要求》（GB/T 20269-2006）

6.《信息安全事件分类分级指南》（GB/Z 20986-2007）

7.《信息安全事件管理指南》（GB/Z 20985-2007）

8.《信息系统灾难恢复规范》（GB/T 20988-2007）

9.《信息安全应急响应计划规范》（GB/T 24363-2009）

五、安全评估内容

本次安全评估内容遵循国家信息安全相关标准及技术规范要求，从物理环境、网络平台、主机层、应用系统等方面，对常州市 12345 平台升级改造项目进行信息安全风险评估，出具安全风险评估报告，明确系统存在的安全隐患、提出整改建议，并在完成安全整改后进行系统复查，出具整改确认报告。

本次信息安全风险评估工作将采用科学的评估手段，对常州市 12345 平台升级改造项目所有应用的建设成果从主机、网络、应用方面进行全面的评估，量化信息安全风险，发现信息安全隐患，为下一步的信息安全决策工作提供基础。

具体内容分类为：物理安全、网络安全、主机安全、应用安全、数据安全、管理安全。

1.物理安全

物理安全主要涉及的方面包括环境安全（防火、防水、防雷击等）设备和介质的防盗窃防破坏等方面。具体包括：物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应和电磁防护。

2.网络安全

网络安全主要关注的方面包括：网络结构、网络边界以及网络设备自身安全等，具体的评估点包括：结构安全、访问控制、安全审计、边界完整性检查、入侵防范、恶意代码防范、网络设备防护。

3.主机安全

主机系统安全涉及的评估点包括：身份鉴别、安全标记、访问控制、可信路径、安全审计、剩余信息保护、入侵防范、恶意代码防范和资源控制。

4.应用安全

应用系统安全的评估点包括：身份鉴别、访问控制、安全审计、剩余信息保护、通信完整性、通信保密性、抗抵赖、软件容错、资源控制、代码安全。

5.数据安全

明确需要保护的数据，评估点包括：数据的保密性、完整性、备份和恢复措施的有效性。

6.管理安全

安全管理制度主要包括：管理制度、制定和发布、评审和修订。

本次评估范围主要涉及主机层和应用层。

六、安全评估过程

1.资产边界分析

（1）分析待评估资产范围；

（2）划分内部资产子系统；

（3）对各子系统进行边界确认；

（4）确定最终资产子系统边界。

2.资产识别

（1）根据资产表格进行资产审计；

（2）分组对本地、非本地区域资产进行有效录入登记；

（3）每类资产明细需要审计资产详细配置与当前状态。

3.威胁识别

（1）从物理准入控制、机房温湿度控制、机房防尘、机房电源、接地、机房屏蔽、以及防雷、防火、防盗等多个方面进行物理威胁识别；

（2）从网络拓扑、地址分配、VLAN划分、路由协议、准入控制、访问控制等多个方面进行网络威胁识别；

（3）从系统来源、系统补丁、账号安全、密码安全、审计安全、服务安全、恶意代码防护等多方面进行系统威胁识别；

（4）从应用服务平台、数据库安全、中间件安全、代码安全、数据安全、账号安全、密码安全、审计安全等多个方面进行应用威胁识别；

（5）从组织架构、人员安全、管理规定、合规性、应用连续性要求等多个方面进行管理威胁识别。

4.脆弱性识别

（1）从物理准入控制、机房温湿度控制、机房防尘、机房电源、接地、机房屏蔽、以及防雷、防火、防盗等多个方面进行物理脆弱性识别；

（2）从系统来源、系统补丁、账号安全、密码安全、审计安全、服务安全、恶意代码防护、日常运维等多方面进行系统脆弱性识别；

（3）从网络拓扑、地址分配、VLAN划分、路由协议、准入控制、访问控制、日常运维等多个方面进行网络脆弱性识别；

（4）从应用服务平台、数据库安全、中间件安全、代码安全、账号安全、密码安全、审计安全、日常运维等多个方面进行应用脆弱性；

（5）从数据备份及恢复、应急响应、灾备与冗余等多方面进行数据脆弱性识别。

5.已有安全措施登记

（1）识别已有操作系统安全策略；

（2）识别已有应用系统安全策略；

（3）识别已有网络系统安全策略；

（4）识别已有安防系统安全策略；

（5）识别已有机房系统安全策略。

6.风险分析

（1）根据收集的用户数据进行分析，评估要素关系映射；

（2）根据评估要素关系进行风险值计算

（3）形成风险评估报告；

（4）针对风险评估报告的解决方案。

7.应用系统渗透性测试

在常州市政务服务管理办公室的授权下，对常州市12345平台升级改造项目进行渗透测试，并提供相关渗透测试报告。

七、提交包括（不限于）以下成果文档

《常州市12345平台升级改造项目弱点评估报告》

《常州市12345平台升级改造项目信息安全风险评估报告》

《常州市12345平台升级改造项目信息安全风险评估复测报告》

附件二：常州市12345平台升级改造项目信息安全风险评估服务项目保密协议

甲方：常州市政务服务管理办公室

乙方：江苏瑞新信息技术股份有限公司

签订日期：2023年09月

为加强甲方常州市12345平台升级改造项目信息安全风险评估服务项目相关系统数据的安全保密管理，贯彻落实《中华人民共和国保守国家秘密法》、《中华人民共和国保守国家秘密法实施办法》、《中华人民共和国网络安全法》《中华人民共和国密码法》等有关法律法规，确保数据的安全保密，促进数据合法、有效利用，防止发生失泄密事件，防范非法使用行为，本着平等、自愿、协商一致、诚实信用的原则，就乙方为甲方网络安全技术支持服务（下称项目）等工作中的保密事宜达成如下协议。

一、 保密信息

（一）在项目中所涉及的项目设计、图片、开发工具、流程图、工程设计图、计算机程序、数据、专利技术、招标文件等内容（在项目中向社会公众提供信息公开和服务的图片、网页、信息数据不包含在内）；

（二）甲方在项目实施中为乙方及乙方工作人员提供必要的数据、程序、用户名、口令和资料等；

（三）甲方在项目实施中涉及的业务及技术文档，包括方案设计细节、程序文件、数据结构，以及相关业务系统的硬软件、文档、测试和测试产生的数据等；

（四）其他甲方合理认为，并告之乙方属于保密的内容。

二、保密范围

（一）甲方已有的技术秘密；

（二）甲方敏感信息和知识产权信息；

（三）乙方持有的科研成果和技术秘密，经双方协商，乙方同意被甲方使用的。

三、保密条款

（一）乙方明确所接收的文件（包括电子和纸质）为甲方所有，甲方拥有以上文件的知识产权。乙方承认甲方在本协议规定的保密信息上的利益和一切有关的权利，乙方应当考虑甲方的利益对该信息予以妥善保存，防止有意或无意的泄漏；

（二）乙方应采取尽可能的措施对所有来自甲方的信息严格保密，包括执行有效的安全措施和操作规程；

（三）甲方为基础数据的管理和提供方，甲方拥有所有数据的全部所有权，乙方需在甲方的授权下使用数据。乙方承诺对甲方以书面、口头、电子文本、电子数据等方式提供的保密信息承担保密义务；

（四）乙方同意仅在为实施本项目时使用保密信息，绝不为与该项目无关的目的使用保密信息；

（五）未经甲方的事先书面批准，乙方不得直接或间接以任何形式或任何方式把保密信息和其中的任何部分，披露或透露给任何第三方（仅可向有知悉必要的乙方内部人员披露，同时仅为甲方项目所需使用）。乙方有义务妥善保管上述文件和数据，不得复制、泄漏或遗失。乙方亦不得依据甲方提供的任何保密信息，就任何问题，向任何第三方作出任何建议；

（六）若乙方确有需要向第三方展示甲方数据信息及成果，需提前向甲方以一事一议的形式提交书面申请，由甲方签字盖章同意后方可施行。未经同意，严禁乙方将甲方数据向第三方展示。如有违反，乙方须承担全部后果，甲方有权向乙方追责；

（七）项目维护过程中，如因业务需要，乙方需采购第三方软件或软件服务的。乙方需以数据最小化为原则，明确数据范围及用途，并与第三方签订数据安全保密协议，确保甲方数据安全；

（八）乙方需加强自身保密意识及保密措施，从管理及技术方面保障甲方数据安全，与员工签订保密协议，约束监督员工，防止个别员工将甲方数据泄露；

（九）乙方的职员违背上述承诺，向第三方披露保密信息，或依据该等保密信息向第三方作出任何建议，都将被视为乙方违反本协议；

（十）甲方保留在甲方认为必要的情况下收回所提供的文件、数据及其使用权的权利；

四、保密信息的所有权

以上所提及的保密信息均为甲方所有。

五、保密期限

（一）本协议的保密期限为5年；

（二）在本协议失效后，如果本协议中包括的某些保密信息并未失去保密性的，本协议仍对这些未失去保密性的信息发生效力，约束双方的行为；

（三）本协议是为防止甲方的保密信息在协议有效期发生泄漏而制定。因任何理由而导致甲、乙双方的合作项目终止时，乙方应归还甲方所有有关信息资料和文件，但并

不免除乙方的保密义务。

六、关系限制

本协议不作为双方建立任何合作关系或其他业务关系的依据。

七、违约责任

乙方未遵守本协议的约定泄露或使用了保密信息甲方有权终止双方的合作项目，乙方应按合作项目金额作为违约金支付甲方，并按照有管辖权的人民法院认定的赔偿金额赔偿甲方遭到的其他损失，甲方有权进一步追究其一切相关法律责任。

八、其他事项

（一）本协议未尽事宜，由甲乙双方协商解决；

（二）本协议自甲、乙双方盖章之日起生效。

甲方：（章）常州市政务服务管理办公室

乙方：（章）江苏瑞新信息技术股份有限公司

附件三：

外包服务网络安全管理承诺书

常州市政务服务管理办公室：

本单位郑重承诺遵守本承诺书的有关条款，如有违反本承诺书有关条款的行为，本单位承担由此带来的一切民事、行政和刑事责任。

一、本单位承诺遵守《中华人民共和国计算机信息系统安全保护条例》和《计算机信息网络国际联网安全保护管理办法》、《网络安全法》《数据安全法》、《个人信息保护法》及有关法律、法规和行政规章制度、文件规定。

二、本单位保证不利用网络危害国家安全、泄露国家秘密，不侵犯国家的、社会的、集体的利益和第三方的合法权益，不从事违法犯罪活动。

三、本单位承诺严格按照国家相关法律法规做好本单位信息安全管理工作，按有关部门要求设立信息安全责任人和信息安全审查员。

四、本单位承诺健全各项网络安全管理制度和落实各项安全保护技术措施。

五、本单位承诺接受公安机关的监督和检查,如实主动提供有关安全保护的信息、资料及数据文件，积极协助查处通过国际联网的计算机信息网络违法犯罪行为。

六、本单位承诺不通过互联网制作、复制、查阅和传播下列信息：

1、反对宪法所确定的基本原则的。

2、危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的。

3、损害国家荣誉和利益的。

4、煽动民族仇恨、民族歧视，破坏民族团结的。

5、破坏国家宗教政策，宣扬邪教和封建迷信的。

6、散布谣言，扰乱社会秩序，破坏社会稳定的。

7、散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的。

8、侮辱或者诽谤他人，侵害他人合法权益的。

9、含有法律法规禁止的其他内容的。

七、本单位承诺不从事任何危害计算机信息网络安全的活动，包括但不限于：

1、未经允许，进入计算机信息网络或者使用计算机信息网络资源的。

2、未经允许，对计算机信息网络功能进行删除、修改或者增加的。

3、未经允许，对计算机信息网络中存储或者传输的数据和应用程序进行删除、修改或者增加的。

4、故意制作、传播计算机病毒等破坏性程序的。

5、其他危害计算机信息网络安全的。

八、本单位承诺，当计算机信息系统发生重大安全事故时，立即采取应急措施，保留有关原始记录，并在 24 小时内向政府监管部门报告，并书面知会贵单位。

九、本单位承诺，管理技术团队相对独立、团队人员为正式员工、专门网络安全负责人。

十、本单位承诺，此项目不得转包、分包合同任务；确需分包的、应报甲方单位同意，并明确相应的网络安全责任和义务，同时明确不得将合同任务主体和关键部分分包。

十一、所有外包活动中产生的政务数据、系统运行数据及收集的个人信息等数据资产归甲方所有。

十二、本单位承诺未经甲方单位同意，不得变更数据用途、用法，不得访问、修改、公开、披露、利用、转让、销毁、私自留存或向第三方提供。

十三、本单位承诺，我单位发生业务转型、合并重组、投资并购等重大事项，或者管理技术团队人员发生重大变化，必须提前向甲方单位报告。

十四、本单位承诺，积极配合相关部门开展网络安全检查、测评、审计等监督管理工作，若是拒绝或不配合监管的追责我单位相关责任。

十五、若违反本承诺书有关条款和国家相关法律法规的，本单位直接承担相应法律责任，造成财产损失的，由本单位直接赔偿。

十六、乙方按规定每年向甲方提交网络安全报告。

十七、本承诺书自签署之日起生效并遵行。

单位盖章：

日　期：2023.9.18